Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-2. (Canceled).

3. (Currently Amended) A method for reprovisioning a token having a first secret, comprising:

sending a request for a certificate;

receiving a certificate that contains a second secret encrypted with a public key of the token, the second secret distinct from the first secret;

decrypting the second secret with a private key of the token;

replacing the first secret with the second secret; and

generating a one time password based on the second ~~secret~~secret,

wherein the second secret is a symmetric cryptographic key.

4. (Previously Presented) The method of claim 3, further comprising, subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret.

5. (Canceled).

6. (Previously Presented) The method of claim 3, wherein the one time password based on the second secret is further based on a personal identification number.

7. (Previously Presented) The method of claim 3, wherein the one time password based on the second secret is further based on a signal from a clock.

8. (Previously Presented) The method of claim 3, wherein the one time password based on the second secret is further based on a counter value.

9. (Currently Amended) A token for generating one time passwords, comprising:

a processor; and

a memory coupled to the processor, the memory storing a first secret and token instructions adapted to be executed by the processor to send a message that includes a request for a certificate, receive a certificate that includes a second secret encrypted with a public key, decrypt the second secret with a private key of the token, ~~store~~replace the first secret with the second secret including storing the second secret in memory, and generate a one time password based on the second ~~secret.~~secret,

wherein the second secret is a symmetric cryptographic key.

10. (Previously Presented) The token of claim 9, further comprising, subsequent to receiving the second secret, discontinuing generation of one time passwords based on the first secret.

11. (Canceled).

12. (Previously Presented) The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on a personal identification number.

13. (Previously Presented) The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on the second secret and a time value.

14. (Previously Presented) The token of claim 9, wherein the token instructions are further adapted to be executed by the processor to generate the one time password based on the second secret and a counter value.

15. (New) The method of claim 3, wherein the certificate is an X.509 certificate.

16. (New) The method of claim 3, wherein the certificate comprises:

a public key received from the token; and

a digital signature based upon a secret asymmetric key of the recipient of the request for the certificate.

17. (New) The token of claim 9, wherein the certificate is an X.509 certificate.

18. (New) The token of claim 9, wherein the certificate comprises:

a public key received from the token; and

a digital signature based upon a secret asymmetric key of the recipient of the request for the certificate.

19. (New) The method of claim 3, wherein the request for a certificate is sent from a PKI enabled device to a PKI certificate authority.

20. (New) A token for generating one time passwords, comprising:

a processor; and

a memory coupled to the processor, the memory separately storing;

a first secret for generating one time passwords;

a private key;

a public key; and

token instructions adapted to be executed by the processor to send a message that includes a request for a certificate, receive a certificate that includes a second secret encrypted with a public key, decrypt the second secret with the private key of the token, replace the first secret with the second secret, and generate a one time password based on the second secret,

wherein the second secret is a symmetric cryptographic key.